UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/527,200	03/10/2005	Yoshikazu Ishii	L9289.05107	2953

24257 7590 02/08/2006

STEVENS DAVIS MILLER & MOSHER, LLP
1615 L STREET, NW
SUITE 850
WASHINGTON, DC 20036

EXAMINER	
AJIBADE AKONAI, OLUMIDE	
ART UNIT	**PAPER NUMBER**
2686	

DATE MAILED: 02/08/2006

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	10/527,200	ISHII, YOSHIKAZU	
	Examiner	Art Unit	
	Olumide T. Ajibade-Akonai	2686	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *10 March 2005*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-9* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-9* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☒ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☒ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☒ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date *3/10/2005*.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

DETAILED ACTION

Claim Rejections - 35 USC § 103

1. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

2. Claims 1-9 are rejected under 35 U.S.C. 103(a) as being unpatentable over **Li et al 20050226423 (hereinafter Li)** in view of **Zhang et al 20040214570 (hereinafter Zhang)**.

Regarding **claims 1 and 5**, Li discloses a wireless LAN access authentication System and method in a network system comprising a plurality of wireless LAN network systems (WLAN cells 1, 2 and 3, see fig. 1, p.1, [0005]) and a center station that controls said plurality o f wireless LAN networks systems in a centralized manner (backbone network, see fig. 1, p.1, [0005]), each said plurality of wireless LAN network systems comprising access point sections (AP11, AP21 and AP31, see fig. 1, p.1, [0005]-[0006]) accessed by a radio terminal apparatus (mobile hosts MHs, see fig. 1, p.1, [0005]) that transmits/receives a radio signal through a radio section and a gateway apparatus which relays transmission/reception of data signals and control signals between said access point sections (wireless gateway 51, 52 and 53, see fig. 1, p.[0005], p.2, [0027]), said center station comprising a center station gateway apparatus that relays transmission/reception of data signals and control signals between the gateway apparatuses of said plurality wireless LAN network systems (inherent, since

the backbone network 4 receives an authentication request containing identity information I and sends property information P to the AP through the wireless gateway, indicating that the backbone network has a gateway through which it routes the information from the authentication server to the wireless gateways of the WLAN cells, see fig. 1, p.2, [0027]) and an authentication server that performs access authentication on said radio terminal apparatus which has accessed said access point sections (authentication server, see p.2, [0025]) and distributes cryptographic keys (key see p.2, [0029]) used for encryption of a radio section through which said access-authenticated radio terminal apparatus carries out communication to said radio terminal apparatus and said access point section (see figs. 1 and 2c, p.2, [0027], [0029]) said wireless LAN access authentication system comprising: an access control section (wireless gateway 51, 52 and 53, see fig. 1, p.1, [0005]) provided for each of said plurality of wireless LAN network systems for controlling the situation of access of said radio terminal apparatus in the own communication area to said authentication server (see figs. 1 and 2a, p.2, [0027]) and checking the presence/absence access of said radio terminal apparatus to said authentication server when said radio terminal apparatus moves to a communication area of a new access point section (see fig. 1, p.1, [0006]); and a cryptographic key control section (AP11, AP21 and AP31, see fig. 1, p.1, [0005]-[0006]) provided for each of said plurality of wireless LAN network systems for controlling cryptographic keys distributed from said authentication server and distributing (see figs. 1 and 2a, p.2, [0027]), when said access control section confirms that said radio terminal apparatus which has moved to the communication area of the other access

point section has already accessed said authentication server, the cryptographic key for said radio section through which said radio terminal apparatus carries out communication to said radio terminal apparatus and said new access point section in the area to which said radio terminal apparatus has moved (see fig. 1, p.1, [0006]).

Li fails to disclose wherein said plurality of wireless LAN network systems comprising at least two access point sections.

In the same field of endeavor, Zhang discloses wherein said wireless LAN network system (wireless LAN 20, see fig. 1, p.1, [0009]) comprising at least two access point sections (APs 18_1-18_4).

It would therefore have been obvious to one of ordinary skill in the art to combine the teaching of Zhang with Li for the benefit of enabling a mobile communications device securely access a wireless LAN.

Regarding **claim 2**, as applied to claim 1, Li further discloses wherein said access control section and said cryptographic key control section are arranged in said gateway apparatus (wireless gateway 51, 52 and 53, see fig. 1, p.1, [0005], p.2, [0027]).

Regarding **claim 3**, as applied to claim 1, Li further discloses wherein access control section (wireless gateway 51, 52 and 53, see fig. 1, p.1, [0005]) comprises a control section that controls at least one access amount of an access time of said radio terminal apparatus or communication packet amount and requests said radio terminal apparatus for reauthentication when said access amount reaches a predetermined amount (inherent, since the communication key between the AP and mobile host is

updated periodically, indicating that the wireless gateways 51-53 will then have to reauthenticate the mobile hosts, see, figs. 33a, 3b, p.3, [0032]-[0035]).

Regarding **claim 4**, Li further discloses wherein said radio terminal apparatus (mobile hosts MHs, see fig. 1, p.1, [0005]) comprises an information card (inherent, since it well known that the mobile host has a SIM card to save information such as identity information I, see fig. 1, p.2, [0025]) which records ID information (identity information I, see fig. 1, p.2, [0025]) and uses the ID information recorded in said information card as an authentication ID at the time access authentication of said radio terminal apparatus (see p.2, [0025]).

Regarding **claim 6**, Li discloses an authentication server (authentication server, see p.2, [0025]) placed in a center station (backbone network, see fig. 1, p.1, [0005]) which carries out access authentication (see p.2, [0025]) of a radio terminal apparatus (mobile hosts MHs, see fig. 1, p.1, [0005]) in a wireless LAN access authentication system in a network system comprising a plurality of wireless LAN network systems (WLAN cells 1, 2 and 3, see fig. 1, p.1, [0005]) and a center station that controls said plurality of wireless LAN network systems a centralized manner, each of said plurality of wireless LAN network systems comprising an access point section accessed by a radio terminal apparatus that transmits/receives a radio signal through a radio section and a gateway apparatus that relays transmission/reception of data signals and control signals between said access point sections (AP11, AP21 and AP31, see fig. 1, p.1, [0005]-[0006]), said center station comprising a center station gateway apparatus that relays transmission/reception of data signals and control signals between the gateway

apparatuses said plurality of wireless LAN network systems (inherent, since the backbone network 4 receives an authentication request containing identity information I and sends property information P to the AP through the wireless gateway, indicating that the backbone network has a gateway through which it routes the information from the authentication server to the wireless gateways of the WLAN cells, see fig. 1, p.2, [0027]), said authentication server comprising: an access authentication section that performs access authentication when said radio terminal apparatus accesses a predetermined access point section of each of said wireless LAN networks (authentication server authenticates the mobile host according to the identity information I, see fig. 2a, p.2, [0027]); and a cryptographic key distribution section that distributes cryptographic keys (key see p.2, [0029]) of a radio section through which said radio terminal apparatus accesses each gateway apparatus of each of said wireless LAN networks all together (see p.2, [0027]).

Li fails to disclose wherein each said plurality of wireless LAN network systems comprising at least two access point sections.

In the same field of endeavor, Zhang discloses wherein said wireless LAN network system (wireless LAN 20, see fig. 1, p.1, [0009]) comprising at least two access point sections (APs 18_1-18_4).

It would therefore have been obvious to one of ordinary skill in the art to combine the teaching of Zhang with Li for the benefit of enabling a mobile communications device securely access a wireless LAN.

Regarding **claim 7**, Li discloses a gateway apparatus (wireless gateway 51, 52 and 53, see fig. 1, p.1, [0005], p.2, [0027]) in each of wireless LAN networks (WLAN cells 1, 2 and 3, see fig. 1, p.1, [0005]) in a wireless LAN access authentication system in a network system (WLAN system, see fig. 1, p.1, [0005]) comprising a plurality of wireless LAN network systems and a center station that controls said plurality of wireless LAN network systems in a centralized manner (backbone network, see fig. 1, p.1, [0005]), each said plurality wireless LAN network systems comprising an access point section accessed by a radio terminal apparatus (mobile hosts MHs, see fig. 1, p.1, [0005]) that transmits/receives radio signal through a radio section (AP11, AP21 and AP31, see fig. 1, p.1, [0005]-[0006]), said center station comprising center station gateway apparatus that relays transmission/reception of data signals and control signals between the gateway apparatuses said plurality wireless LAN network systems (inherent, since the backbone network 4 receives an authentication request containing identity information I and sends property information P to the AP through the wireless gateway, indicating that the backbone network has a gateway through which it routes the information from the authentication server to the wireless gateways of the WLAN cells, see fig. 1, p.2, [0027]) and an authentication server (authentication server, see p.2, [0025]) that performs access authentication on said radio terminal apparatus which has accessed said access point section (authentication server authenticates the mobile host according to the identity information I, see fig. 2a, p.2, [0027]) and distributes cryptographic keys (key see p.2, [0029]) used for encryption of a radio section through which said access-authenticated radio terminal apparatus carries out communication to

said radio terminal apparatus and said access point section, said gateway apparatus comprising: transmission/reception section that transmits/receives said data signals and said control signals to/from the center station gateway apparatus said center station (wireless gateway 51, 52 and 53, see fig. 1, p.1, [0005], p.2, [0027]); an access control section that controls the situation of access of said radio terminal apparatus to said authentication server within each of said wireless LAN networks and checks the presence/absence of access of said radio terminal apparatus to said authentication server when said radio terminal apparatus moves to a communication area of a new access point section (see fig. 1, p.1, [0005]); and a cryptographic key control section that controls said cryptographic keys distributed from said authentication server through said access control section and distributes, when it is confirmed that said radio terminal apparatus which has moved to the communication area of the other access point section has already accessed said authentication server, said cryptographic key for the radio section through which said radio terminal apparatus carries out communication to said radio terminal apparatus and the new access point section the area to which said radio terminal apparatus has moved (see fig. 1, p.1, [0006], p.2, [0027]).

Li fails to disclose wherein each said plurality of wireless LAN network systems comprising at least two access point sections.

In the same field of endeavor, Zhang discloses wherein said wireless LAN network system (wireless LAN 20, see fig. 1, p.1, [0009]) comprising at least two access point sections (APs 18_1-18_4).

It would therefore have been obvious to one of ordinary skill in the art to combine the teaching of Zhang with Li for the benefit of enabling a mobile communications device securely access a wireless LAN.

Regarding **claim 8**, as applied to claim 7, Li further discloses wherein said access control section (wireless gateway 51, 52 and 53, see fig. 1, p.1, [0005]) comprises a control section that controls at least one access amount of an access time of said radio terminal apparatus or communication packet amount and requests said radio terminal apparatus for reauthentication when said access amount reaches a predetermined amount (inherent, since the communication key between the AP and mobile host is updated periodically, indicating that the wireless gateways 51-53 will then have to reauthenticate the mobile hosts, see, figs. 33a, 3b, p.3, [0032]-[0035]).

Regarding **claim 9**, Li discloses a radio terminal apparatus (mobile hosts MHs, see fig. 1, p.1, [0005]) used in a wireless LAN access authentication system in a network system (WLAN system, see fig. 1, p.1, [0005]) comprising a plurality of wireless LAN network systems (WLAN cells 1, 2 and 3, see fig. 1, p.1, [0005]) and a center station (backbone network, see fig. 1, p.1, [0005]) which controls said plurality of wireless LAN network systems in a centralized manner, each of said plurality of wireless LAN network systems comprising an access point section accessed by a radio terminal apparatus transmitting/receiving a radio signal through a radio section and a gateway apparatus that relays transmission/reception of data signals and control signals between said access point sections (AP11, AP21 and AP31, see fig. 1, p.1, [0005]-[0006]), said center station comprising a center station gateway apparatus that

relays transmission/reception of data signals and control signals between the gateway apparatuses of said plurality of wireless LAN network systems (inherent, since the backbone network 4 receives an authentication request containing identity information I and sends property information P to the AP through the wireless gateway, indicating that the backbone network has a gateway through which it routes the information from the authentication server to the wireless gateways of the WLAN cells, see fig. 1, p.2, [0027]) and an authentication server that performs access authentication on said radio terminal apparatus which has accessed said access point section (authentication server authenticates the mobile host according to the identity information I, see fig. 2a, p.2, [0027]) and distributes the cryptographic key (key see p.2, [0029]) used for encryption of the radio section through which said access-authenticated radio terminal apparatus carries out communication to said radio terminal apparatus and said access point section, said radio terminal apparatus comprising an information card (inherent, since it well known that the mobile host has a SIM card to save information such as identity information I, see fig. 1, p.2, [0025]) in which ID information (identity information I, see fig. 1, p.2, [0025]) is recorded when access authentication is performed by said authentication server of said center station (see p.2, [0025]).

Conclusion

3. The prior art made of record and not relied upon is considered pertinent to applicant's disclosure.

Wild et al (20040181692) discloses a method and apparatus for providing network service information to a mobile station by a wireless local area network.

Whelan et al (20030219129) discloses a system and method for providing WLAN security through synchronized update and rotation of WEP keys.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Olumide T. Ajibade-Akonai whose telephone number is 571-272-6496. The examiner can normally be reached on M-F, 8.30p-5p.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Marsha D. Banks-Harold can be reached on 571-272-7905. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

OA

CHARLES APPIAH
PRIMARY EXAMINER